PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-227870

(43)Date of publication of application : 15.08.2000

(51)Int.Cl. G06F 12/00
G06F 13/00
G06F 17/30

(21)Application number : 11-316360

(22)Date of filing : 08.11.1999

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>

(72)Inventor : BACHA HAMID
CARROLL ROBERT BRUCE
MIRLAS LEV
TCHAO SUNG WEI

(30)Priority

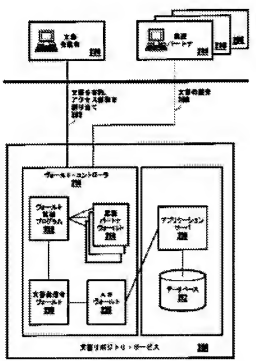
Priority number : 98 2256936 Priority date : 23.12.1998 Priority country : CA

(54) SYSTEM FOR RETRIEVING ELECTRONIC DATA FILE AND MAINTENANCE METHOD THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system for enabling an entity, for which access to a document in a data repository is permitted by a transmitter of the document, to retrieve the document preserved in the repository of a third person in safe.

SOLUTION: A document transmitter 200, a repository manager and all the entities having the privilege of access to data in the repository have vault environments as the safe expansion of respective work areas. A vault of the document transmitter 200 maintains an access control list(ACL) concerning the respective documents stored in the repository. The vault of each entity having the privilege of access to any arbitrary document in the repository maintains a function list collecting the



privileges of access to all the documents stored in the repository of the entity.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－227870
（P2000－227870A）
(43)公開日　平成12年８月15日(2000.8.15)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ		テーマコード*（参考）
Ｇ０６Ｆ　12/00	５３７	Ｇ０６Ｆ	12/00	５３７Ａ
13/00	３５４		13/00	３５４Ｄ
17/30			15/40	３１０Ｆ
				３２０Ａ

審査請求　有　　請求項の数12　ＯＬ　（全 20 頁）

(21)出願番号　特願平11－316360

(22)出願日　平成11年11月８日(1999.11.8)

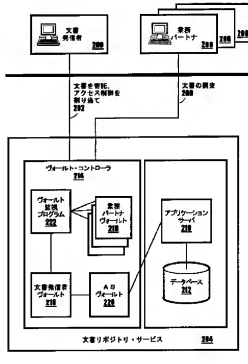
(31)優先権主張番号　２２５６９３６
(32)優先日　平成10年12月23日(1998.12.23)
(33)優先権主張国　カナダ（ＣＡ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(74)代理人　100086243
弁理士　坂口　博　（外１名）

最終頁に続く

(54)【発明の名称】　電子データ・ファイルを検索するシステムおよびその維持方法

(57)【要約】
【課題】　文書の発信者によってデータ・リポジトリ内の文書へのアクセスを許可されたエンティティが、第三者のリポジトリに保管されている文書を安全に検索できるシステムを提供すること。
【解決手段】　文書発信者、リポジトリ管理者、およびリポジトリ内のデータに対するアクセス特権を有するすべてのエンティティは、それぞれの作業領域の安全な拡張であるヴォールト環境を有する。文書発信者のヴォールトは、リポジトリに格納した各文書に関するアクセス制御リスト（ＡＣＬ）を維持する。リポジトリ内にある任意の文書に対するアクセス特権を有する各エンティティのヴォールトは、エンティティのリポジトリ内に格納されているすべての文書に対するアクセス特権をまとめた機能リストを維持する。



【特許請求の範囲】
【請求項１】データ・リポジトリ・システムに格納された電子データ・ファイルを検索するための安全なシステムであって、
（ｉ）データ・リポジトリ・システム内にある電子データ・ファイルの寄託側コンピュータ用の第１のエージェント・プログラムと、
（ｉｉ）電子データ・ファイルへのアクセス特権を有する第１のユーザ・コンピュータ用の第２のエージェント・プログラムとを収容する通信環境と、
前記第１のエージェント・プログラムによってアクセス可能であり維持され、電子データ・ファイルに関するアクセス制御をリストした電子データ・ファイルの目録と、
前記第２のエージェント・プログラムによってアクセス可能であり維持され、電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権に関する第１の記録と、
電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、第１の記録を更新するため、前記第１のエージェント・プログラムから前記第２のエージェント・プログラムへ伝える手段と、
電子データ・ファイルが前記第２のエージェント・プログラムに解放される前に、前記第１のエージェント・プログラムが電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権を検証するための手段とを含むシステム。
【請求項２】前記第１のエージェント・プログラムが寄託側コンピュータの安全な拡張であり、前記第２のエージェント・プログラムが第１のユーザ・コンピュータの安全な拡張である、請求項１に記載の安全なシステム。
【請求項３】電子データ・ファイルに対する前記第１のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、前記第２のエージェント・プログラムから第１のユーザ・コンピュータへ伝える手段をさらに含む、請求項２に記載の安全なシステム。
【請求項４】電子データ・ファイルに対するアクセス特権を有する第２のユーザ・コンピュータ用の第３のエージェント・プログラムと、
前記第３のエージェント・プログラムによってアクセス可能であり維持され、電子データ・ファイルに対する第２のユーザ・コンピュータのアクセス特権に関する第２の記録とを含み、
第１の記録を更新するために、電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、前記第１のエージェント・プログラムから前記第２のエージェント・プログラムへ伝える手段が、第２の記録を更新するために、電子データ・ファイルに対する第２のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、前記第１のエージェント・プログラムから前記第３のエージェント・プログラムに伝える手段を含み、
電子データ・ファイルが前記第２のエージェント・プログラムに解放される前に、前記第１のエージェント・プログラムが電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権を検証するための手段が、電子データ・ファイルが前記第３のエージェント・プログラムに解放される前に、前記第１のエージェント・プログラムが電子データ・ファイルに対する第２のユーザ・コンピュータのアクセス特権を検証するための手段を含む、請求項１または２にいずれか一項に記載の安全なシステム。
【請求項５】前記第３のエージェント・プログラムが前記第２のユーザ・コンピュータの安全な拡張である、請求項４に記載の安全なシステム。
【請求項６】電子データ・ファイルに対する前記第２のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、前記第３のエージェント・プログラムから前記第２のユーザ・コンピュータに伝える手段をさらに含む、請求項５に記載の安全なシステム。
【請求項７】通信環境がサーバを含む、請求項２または５に記載の安全なシステム。
【請求項８】前記通信環境に収容されたデータ・リポジトリ・システムへのインタフェースをさらに含み、前記インタフェースがデータ・リポジトリ・システムおよびエージェント・プログラムとの間の双方向通信をすべて受け取るように適合されている、請求項１、２、または５のいずれか一項に記載の安全なシステム。
【請求項９】前記インタフェースが前記データ・リポジトリ・システムの安全な拡張である、請求項８に記載の安全なシステム。
【請求項１０】電子データ・リポジトリ用の安全な電子データ検索システムを維持する方法であって、前記システムが、データ・リポジトリ内に格納された各電子データ・ファイルに関するアクセス制御をリストした目録と、リポジトリ内に格納された電子データに対するアクセス権を有する各コンピュータの文書アクセス特権をリストした記録とを有し、
リポジトリ内に格納されている電子データ・ファイルに関する目録を更新するステップと、
前記更新によって電子データ・ファイルへのアクセスが変更されたすべてのコンピュータを識別するステップと、
前記アクセスの変更を影響されるすべてのコンピュータに伝えるステップと、
影響されるすべてのコンピュータのアクセス特権記録を更新するステップと、
前記更新されたアクセス特権記録を前記影響されるコンピュータに伝えるステップとを含む方法。

【請求項１１】データ・リポジトリ・システム内に格納された電子データ・ファイルを検索するための安全なシステムであって、
データ・リポジトリ・システム内に格納された各電子データ・ファイルに関するアクセス制御をリストした目録を維持する手段と、
各目録へのアクセスを寄託特権を有するコンピュータだけに制限する手段と、
データ・リポジトリ・システム内の少なくとも１つの電子データ・ファイルへのアクセス特権を有する各コンピュータに関連付けられた電子データ・ファイルに対するアクセス特権をリストした記録を維持する手段と、
前記各記録に対するアクセスを前記アクセス特権を有する関連するコンピュータだけに制限する手段と、
目録のアクセス変更によって影響を受ける各コンピュータに関連付けられた前記記録を更新する手段とを含むシステム。
【請求項１２】請求項１０に記載の方法をコンピュータで実行する際に使用するための命令を格納するコンピュータ可読メモリ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子データ格納の分野を対象とし、さらに詳細には、データ検索時および取出し時にアクセス制御が実施され第三者であるデータ保管者（custodian）によって管理される、安全なデータ・リポジトリ／交換システムを提供する。
【０００２】
【従来の技術】ネットワーク通信と公開キー・インフラストラクチャ（public key infrastructure）（「ＰＫＩ」）テクノロジにおける最近の平行した進歩によって、企業や公的機関は、あらゆる種類の記録保管および業務処理に際して、電子文書を使用するようになってきた。伝送の保全性および機密保護の向上に伴い、インターネットや他のオープン・ネットワークを介して電子的に送信される文書は、改ざんされずに完全な形で着信すると確信することができる。データベース管理システムを、数ギガバイトのデータを記憶することができる最新のコンピュータ・メモリと組み合わせることによって、企業や公的機関は、不動産コストのかさむ大量の記録用紙を保管しなくてもよくなった。
【０００３】一般に、１つのエンティティから発信されるデータは、寄託、検討などいくつかの理由で他のエンティティへ送信しなければならないことがある。このデータ要素は、銀行口座やその他の財務情報など非構造化文書ファイルまたは構造化レコードの形式を採ることができる。非構造化データの例では、検討の目的で、発信元システムから同じシステム内の他のコンピュータへ、または別のシステム上に常駐するコンピュータへ、文書を転送する必要が生じることがある。こうした状況は、企業の立場（たとえば、合弁事業の申込みや複雑な入札の目的）においても、公的機関の立場（たとえば大学の論文審査委員会に提出する前に指導教官によって検討される卒業論文）においても、等しく発生する可能性がある。文書は（特に長い文書の場合）、毎回文書全体をタイプし直す必要がなく、改訂や追加が容易にできるので、電子的に作成されている。
【０００４】文書を電子形式にすると簡単に伝送できることから、検討も容易になる。所期の検討者は文書の格納場所へのアクセス権を与えられると、システムを検索することによってその文書が使用可能であることを発見することができる。
【０００５】文書をローカルに格納することがファイアウォールの背後にいる第三者にアクセス権を提供することを意味する場合、文書の作成者がこのような格納を望まないのには、機密保護、データの保全性、およびシステムまたはネットワークの可用性など、いくつかの理由がある。これらの理由については、本発明者等が同時に提出し本願と同じ譲受人に譲渡された「System for Electronic Repository of Data Enforcing Access Control on Data Retrieval」という名称の特許出願（ＩＢＭ整理番号第ＣＡ９９８－０３０号）により詳細に記載されており、この出願は、参照により本明細書に組み込まれる。
【０００６】本発明者等が同時に提出した出願は、リポジトリに格納されたデータへの保全性およびアクセスが、そのリポジトリの第三者である管理者が行うどんなアクションとも無関係に維持されるシステムを対象とする。
【０００７】前記出願に記載された発明は、文書に対する許可されたユーザ・アクセスに関する情報が単一の中央位置、すなわちリポジトリ自体に格納されているため、多数のユーザがアクセス可能な多数の文書を含むシステムの場合に非常に効率がよい。ユーザは、システム外部の手段によって文書への自分のアクセスに関する安全な知識を得る。
【０００８】本発明は、許可されたユーザ・アクセスに関する情報をシステム自体に格納するという修正であり、これもリポジトリの第三者である管理者のどんなアクションからも保護されている。
【０００９】
【発明が解決しようとする課題】したがって、本発明の一目的は、第三者によって管理されるリポジトリ内に物理的に格納されるどの文書に対してアクセス権を有するかを判定するために検索することができる電子文書の格納および交換システムを提供することである。
【００１０】本発明の他の目的は、リポジトリに格納されたデータに対する許可されたユーザ・アクセスに関する情報への保全性およびアクセスがそのシステムを介して使用可能であるが、第三者のリポジトリ管理者のアク

ションには依存しないシステムを提供することである。

【００１１】

【課題を解決するための手段】したがって、一態様において、本発明は電子データ・リポジトリ・システムに格納された電子データ・ファイルを検索するための安全なシステムを提供する。このシステムは、データ・リポジトリ・システム内にある電子データ・ファイルの寄託側コンピュータ用の第１のエージェント・プログラムと、その電子データ・ファイルへのアクセス特権を有する第１のユーザ・コンピュータ用の第２のエージェント・プログラムとを収容する通信環境を含む。電子データ・ファイルの目録には、電子データ・ファイルに関するアクセス制御がリストされる。この目録は第１のエージェント・プログラムによってアクセス可能であり維持される。第１のユーザ・コンピュータは、第２のエージェント・プログラムによってアクセス可能であり維持される電子データ・ファイルに対するそれ自体のアクセス特権の記録を有する。電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権に影響を与えるような目録の変更が行われた場合、これらの変更が第１のエージェント・プログラムから第２のエージェント・プログラムに伝えられ、第１のユーザ・コンピュータのアクセス特権を更新することができる。第１のエージェント・プログラムはまた、第１のユーザ・コンピュータの電子データ・ファイルが第２のエージェント・プログラムに解放される前に、この電子データ・ファイルに対するアクセス特権を検証することができる。

【００１２】別の態様によれば、本発明は、データ・リポジトリ内に格納された各電子データ・ファイルに関するアクセス制御をリストした目録と、リポジトリ内に格納された電子データに対してアクセス権を有する各コンピュータの文書アクセス特権をリストした記録とを有するシステム内で、電子データ・リポジトリの電子データを安全に検索するのを維持する方法を提供する。この方法は、リポジトリ内に格納されている電子データ・ファイルに関する目録を更新するステップと、この更新によって影響を受ける電子データ・ファイルへのアクセスが変更されるすべてのコンピュータを識別するステップと、このアクセスの変更を影響を受けるすべてのコンピュータに伝えるステップと、影響を受けるすべてのコンピュータのアクセス特権記録を更新するステップと、更新されたアクセス特権記録を影響を受けるコンピュータに伝えるステップからなる。

【００１３】さらに別の態様によれば、本発明は、データ・リポジトリ・システム内に格納された各電子データ・ファイルに関するアクセス制御をリストした目録を維持する手段と、各目録へのアクセス権を寄託特権を有するコンピュータだけに制限する手段と、データ・リポジトリ・システム内の少なくとも１つの電子データ・ファイルへのアクセス特権を有する各コンピュータに関連付けられた電子データ・ファイルに対するアクセス特権をリストした記録を維持する手段と、前記各記録に対するアクセス権をこのアクセス特権を有する関連付けられたコンピュータだけに制限する手段と、目録のアクセス変更によって影響を受ける各コンピュータに関連付けられた記録を更新する手段とを含む、データ・リポジトリ・システム内に格納された電子データ・ファイルを検索するための安全なシステムを提供する。

【００１４】本発明では、上記システムまたは方法を実行するプログラム・コードで符号化された媒体も提供される。

【００１５】

【発明の実施の形態】第三者の保管者を利用する文書リポジトリ・システムの従来の配置を図１に示す。文書発信者１００は、その接続１０２を介して、第三者によって管理されるデータベースなどのリモート文書リポジトリ・サービス１０４に文書を預けることができる。寄託文書の所有者として、文書発信者１００はその文書へのアクセスを割り当てることができる。たとえば、文書発信者は、業務パートナ１０６に「読取り」権限を割り当てることが可能であるが、これは、割り当てられた業務パートナがその文書リポジトリ・サービス１０４への接続１０８を介して文書を取り出すことができるが、寄託文書を変更することはできないという意味である。

【００１６】このような従来のシステムでは、一般に、要求時に業務パートナ１０６が文書を検討できるように、文書発信者１００から寄託された文書は暗号化されない。これは、従来技術では文書の暗号解読に関連した問題があるためである。文書を暗号解読するには、文書発信者１００の秘密キーにアクセスする必要がある。秘密キーにアクセスするには、文書発信者１００が、暗号解読自体を実行するために暗号解読が要求される可能性のある場合にはいつでも自分自身をオンラインで使用できるようにしておく（システム可用性の問題）か、またはその秘密キーを業務パートナ１０６が直接または信用される代理人（図示せず）を介して使用できるようにするためにあらかじめスキームをセットアップしておく必要がある。

【００１７】インターナショナル・ビジネス・マシーンズ・コーポレイションの米国特許第５４９１７５０号は、「Method and Apparatus for Three-Party Entity Authentication and Key Distribution Using Message Authentication Codes」に関するものである。この特許は、２者またはそれ以上の通信パートナが信用される仲介者を介して認証された後に、この通信パートナによって共用される秘密のセッション管理キーの配布を可能にするシステムについて記載している。ただし、このスキームの下で生成されたキーならびにこれと同様の他のキーは一時的なものであって、絶対に必要な場合以外はほとんど使用しないように意図されている。このようなス

キーが、永続的な文書リポジトリを使用した文書検討システムで、通信パートナ間での暗号解除キーの安全な伝送を行うのに適しているかどうかは明らかでない。

【００１８】したがって、文書が一定期間寄託され暗号化されない従来のシステム（図１）では、第三者の管理者であるリポジトリ・サービス１０４は文書の保全性維持について信用できるものでなければならない。

【００１９】本発明の好ましい実施形態の文書リポジトリ・システムは、ＩＢＭ社に譲渡された１９９７年１１月２６日出願の「Secure Server and Method of Operationfor a Distributed Information System」という名称の、米国特許出願第９８００２２号の主題である、IBM Vault Registry製品を使用して構築することができる。米国特許出願第９８００２２号は参照により本明細書に組み込まれる。IBMVault Registry製品は、ヴォールト（Vault）と呼ばれるクライアント環境の安全な拡張を実装する、拡張ｗｅｂサーバ環境を提供する。このシステムは、電子的に伝送される文書および他のデータがそのままの形でエラーもなく着信するという、本明細書の発明の属する技術分野に記載した最新の伝送技術を利用している。クライアントのヴォールト内に含まれるリソースは、認定された公開キーによる強力な認証を使用してクライアントからアクセスされた場合にのみ使用可能となる。環境によっては、クライアントのｗｅｂブラウザを介してアクセスすることもある。

【００２０】ヴォールトの情報内容は、プライバシーのため暗号化されている。サーバ上にあるヴォールトは、固有の暗号キー、およびブラウザを介したアクセスなどヴォールトの所有者によって承認された信用できる経路を介したアクセス以外のキーへのアクセスを抑制する機構を有する。ヴォールト内で実行されるプログラムは、以下のことを保証するために、オペレーティング・システム・サービスによって分離されている。

ａ）ヴォールト内で動作するプログラムによる改変の可能性なしに従属プロセスにその識別が使用できるように、システム識別（仮想ログオン）を使用したプロセスで動作する。

ｂ）その中で動作しているヴォールトのデータ内容だけにアクセスでき、他のものにはアクセスできない。

ｃ）ヴォールトの所有者によって、ヴォールト内での実行が承認されている。

ｄ）改ざんや「トロイの木馬」攻撃を防ぐために署名されている。

【００２１】ヴォールト内で動作するプログラムは、同じヴォールト、または互いの公開キーへの安全なアクセスを有する他のヴォールトに情報を預けることができる。一般に、これらのヴォールトは同じヴォールト・サーバ上に配置されているが、異なるヴォールト・サーバ上に配置し、公開キー情報を提供するために共通の認証機関にアクセスすることもできる。ヴォールト・リポジトリの文脈では、「寄託」という語が様々な意味を持つことがある。一実施態様では、寄託という語は目標ヴォールトの暗号化キーにデータを暗号化し、そのデータを寄託ヴォールトの署名キー中で署名することを表すことができる。ヴォールト・プログラムは、暗号化キーと署名キーのどちらにも直接アクセスすることはできない。これは、ＡＰＩを介して実行される。任意選択で、「寄託」機能は、目標ヴォールト内に収容されている待ち行列に情報を入れることもできる。別のオプションでは、情報が寄託されたこと、および目標ヴォールト内のプログラムがデータをオープンしたことを確認する「配達証明（return receipt）」が提供される。これらすべての「寄託」機能は、次のような形でヴォールト内で情報を受け渡す手段を提供する。

ａ）元のプロセスは否定できない。

ｂ）プロセス間通信バッファを検査する機能を有するものによって、内容が閲覧されない。

ｃ）送達が保証されている。

【００２２】アプリケーションが目標ヴォールトへのデータを待ち行列に入れることを選択しない場合は、ファイル、データベース、あるいはデータを「不透明な（opaque）」項目として処理できる（たとえばオブジェクトが永続性になるようにシリアル化する）他の任意のシステム・サービスを使用して、情報を格納することを選択することができる。この不透明情報は、バックアップおよび回復用の標準的なシステム技術で管理することができる。ただし、その内容は、SecureDepositorアプリケーション・プログラミング・インタフェースを使用してそれを所有するヴォールトの文脈で実行されるプログラムによってのみ、暗号解読することができる。

【００２３】IBM Vault Registry製品を使用した本発明の好ましい実施形態を、図２に略図で示す。

【００２４】図１に示したシステムと同様に、図２に示したスキームでは、文書発信者２００が文書リポジトリ・サービス２０４との接続２０８を介して文書を寄託することができ、さらに寄託文書の所有者として、業務パートナなどの第三者２０６に、その文書へのアクセス・レベルを割り当てることができ、この第三者２０６は、自分自身のネットワーク接続２０８を介して文書リポジトリ・サービス２０４内にある文書へアクセスできるようになる。ただし、前述のシステムとは異なり、文書リポジトリ・システムのユーザには、第三者を信用してリポジトリ内の文書フィールドの保全性を維持させる義務はない。

【００２５】好ましい実施形態の文書リポジトリ・システム２０４は、２つの構成要素、アプリケーション・サーバ２１０およびヴォールト・コントローラ２１４を備える。アプリケーション・サーバ（ＡＳ）は、データベース・リポジトリ２１２を管理するプログラムであって、同じマシン上にあっても、また閉じたネットワーク

上のリモート位置にあってもよい。ヴォールト・コントローラ２１４は、複数の構成要素、すなわち個別に文書発信者２００および業務パートナ２０６に割り当てられたユーザ・ヴォールト２１６、２１８、アプリケーション・サーバ２１０に割り当てられたＡＳヴォールト２２０、ならびにヴォールト監視プログラム２２２を含む。

【００２６】ユーザ・ヴォールト２１６または２１８には、適切な認証に基づいてヴォールトが割り当てられたユーザ（文書発信者２００または業務パートナ２０６）だけがアクセスすることができる。個々のヴォールトは文書データベース２１２に直接アクセスすることができず、アクセスはＡＳヴォールト２２０およびアプリケーション・サーバ２１０を介して行われる。

【００２７】アプリケーション・サーバ構成要素２１０は、信用されるコンピューティング・ベースでは実行されないが、任意のプラットフォーム上で実行可能である。アプリケーション・サーバは、ヴォールト・サーバ２１４内にあるこれに割り当てられたＡＳヴォールト２２０内で実行される交互（reciprocating）構成要素を有する。ＡＳヴォールト２２０はアプリケーション・サーバ２１０と通信可能であり、このアプリケーション・サーバを介して文書データベース２１２にアクセスすることができる。

【００２８】図３は、本発明の好ましい実施形態による、文書作成のプロセスを示す流れ図である。IBM Vault Registry環境を使用すると、パーソナル・ヴォールトは概念的にヴォールト所有者環境の安全な拡張となる。したがって、図３では、文書発信者とアプリケーション・サーバのヴォールト間での各プロセス・ステップ間の対話が示されている。

【００２９】データ・リポジトリ内で文書を作成する場合、文書はまずこれを作成または発信したユーザのデスクトップからユーザ（文書発信者）のパーソナル・ヴォールトに送信され（ブロック３００）、ここで文書はユーザ・ヴォールトの秘密署名キーで「署名」される（ブロック３０２）。

【００３０】データ要素の電子署名とは、署名者がその データ要素の保全性を保証するものである。署名は、まずデータ要素のダイジェストを計算することにより算出することができる。このダイジェストは、セキュリティを保証するための特有のプロパティを有する、比較的小規模な構造（たとえば、ＭＤ２またはＭＤ５ダイジェストの場合１２８ビット）である。第１に、これは一方向関数であり、すなわちダイジェストが与えられても、それを生成したオリジナル文書を取得することは不可能である。さらに、ダイジェストが与えられても、同じダイジェストを有するはずの第２のプレイメージを見つけることも不可能（または計算による実現不可能）である。ダイジェストは、衝突に対する耐性もある。すなわち、２つの異なるプレイメージが同じダイジェストを生成することはほとんどあり得ない。

【００３１】次いでデータ要素のダイジェストは、ユーザ・ヴォールト・アプリケーションの秘密署名キーを使って暗号化される（ブロック３０４）。好ましい実施形態では、対称暗号技術および公開キー非対称暗号技術の両方が使用される。

【００３２】公開キー暗号を使用する場合、アプリケーションは、キー・ペアと呼ばれる公開キーと秘密キーの２つのキーを有する。秘密キーはアプリケーションによってローカルに保持されており、下記で詳しく論じる。公開キーは、通常はＸ．５００分散型ディレクトリのようなディレクトリ・サービスを介して、すべてのユーザが使用できるようになっている。公開キー配布は、当技術分野で周知であり、本明細書ではこれ以上詳しくは論じない。

【００３３】公開キー暗号が使用されるとき、公開キーで暗号化されたデータ要素は、対応する秘密キーでのみ暗号解読することができる。同様に、秘密キーで暗号化されたデータ要素は、公開キーでのみ暗号解読することができる。

【００３４】対称キー技法では、暗号化と暗号解読の両方に１つのキーが使用される。現在のところ、対称キー技法による暗号化／暗号解読およびキー生成の方が公開キー非対称技法を用いるよりもかなり高速である。

【００３５】データは通常、ランダムに生成された対称キーを使用して暗号化される。次いでこの対称キーは、ユーザの公共暗号キーを使用してそれ自体が暗号化され文書と共に格納されて、文書の一部となる。

【００３６】さらに図３を続けて見ていくと、暗号化された文書と電子署名は、文書データベースに保管するためにアプリケーション・サーバのヴォールトに転送される（ブロック３０６）。暗号化された文書を受け取ると（ブロック３０８）、アプリケーション・サーバのヴォールト内で実行中のアプリケーションは、それ自体の秘密署名キーを使用して再署名することによって、署名を公証する（ブロック３１０）。

【００３７】電子的文脈において、署名の公証とは、「公証人」としての役割を果たす第三者が、署名の内容を証明するという意味である。（政府機関によって授与された公証人役場に課せられたすべての義務が、本明細書における「公証人」および「公証」の参照によってカバーされるものではない。）一般に署名の電子公証は、後でその署名が許可なく修正されるのを防ぐための特別な予防措置として実行される。本発明の場合、ユーザのデジタル署名の公証は、ユーザが文書リポジトリ内にあるオリジナル文書を置き換えたり修正したりするのを防ぐ。その文書に関連する公証済み署名をチェックすれば、不一致があれば明らかになるはずである。

【００３８】公証済みの電子署名には、所与のデータ要素の発信者署名とその発信者署名の公証人の署名という

２つの情報が含まれる。公証人の署名は、発信者署名および現タイム・スタンプに関して計算されるものとする。

【００３９】その後アプリケーション・サーバのヴォールト内で実行中のアプリケーションは、受け取った文書に署名する（ブロック３１２）。文書発信者から受け取ったデータは暗号化されているため、アプリケーション・サーバは実際には文書の内容について何の知識も持たない。したがって、本発明によれば、この第２の署名は暗号化文書および発信者の公証済み署名に対して計算される。アプリケーション・サーバの署名は、リポジトリ・サービスが文書を受け取ったことを文書発信者（寄託元）に対して証明する、非拒否証明（non-repudiation receipt）となる。その後リポジトリ内で文書を作成しても、後でリポジトリ・サービスによって拒否されることはない。

【００４０】暗号化された文書、文書発信者の公証済み署名、および非拒否証明は、すべてアプリケーション・サーバのリポジトリまたはアプリケーション・データベースに格納される（ブロック３１４）。非拒否証明は、文書発信者のヴォールトに送信される（ブロック３１６）。文書発信者のヴォールトは、暗号化された文書の署名を検証することにより、非拒否証明の正確さをチェックする（ブロック３１８）。文書発信者のヴォールトはまた、公証済み署名のタイム・スタンプが現在のものであるかどうかをチェックする（ブロック３２０）。タイム・スタンプの許容範囲は、アプリケーションに依存する。これらのテストのどちらかに不合格になると、エラー・メッセージがＡＳヴォールトに戻され（ブロック３２２）、システムに記録される。証明が正しい現在のものであれば、ユーザのヴォールト内で実行されているアプリケーションは、文書がリポジトリに格納されているとの証明が必要になった場合、非拒否証明を将来の参照用にローカルに保管しておくために発信者ユーザに戻す（ブロック３２４）。

【００４１】文書発信者は、格納のためにヴォールトに提出する前に、自分の知的所有権のある技法を使用して文書の署名または暗号化あるいはその両方を行うことができる。ただし、文書リポジトリは、格納される文書の内容に関知しない。したがって、暗号化された文書は、他の文書が処理されるのと同様に、ユーザのヴォールトによって再署名および再暗号化される。

【００４２】図４は、本発明の好ましい実施形態による、アクセス制御リスト（ＡＣＬ）と呼ばれる各文書について文書発信者が維持する一種の目録に従って許可された要求元による文書の取出しを許可する際に実行しなければならないステップを示す流れ図である。図３と同様に、このプロセス・ステップは、各パーソナル・ヴォールトがそれぞれの作業領域の概念的に安全な拡張であることに基づいて、ユーザ、アプリケーション・サーバ、および要求元の３者の間で分割されている。

【００４３】図４から始めると、要求元が自分のヴォールト・アプリケーションに対して、アプリケーション・サーバ・リポジトリから文書を取り出すように要求し（ブロック４００）、要求元のヴォールト・アプリケーションがその文書に対する要求を、アプリケーション・サーバのヴォールトに転送する（ブロック４０２）。

【００４４】アプリケーション・サーバのヴォールト・アプリケーションは、アクセス要求を受け取り（ブロック４０４）、暗号化文書および発信者の公証済み署名を、アプリケーション・データベースから取り出す（ブロック４０６）。

【００４５】アプリケーション・サーバのヴォールト・アプリケーションは、暗号化文書および公証済み署名を文書発信者のヴォールトに送信する。アプリケーション・サーバのヴォールトはまた、要求元のヴォールトの識別を発信者のヴォールトに送信する（ブロック４０８）。

【００４６】発信者のヴォールトは、要求元が文書を取り出す許可を与えられていることをチェックする（ブロック４１０）。好ましい実施形態では、文書アクセス制御は、文書アクセスを許可されたエンティティだけに制限する際に使用されるアクセス制御リストを介して実行可能になる。アクセス制御リスト（ＡＣＬ）は文書に関連付けられており、図６および図８に関連して下記に記載するように、文書発信者のヴォールト内に格納され維持される。要求元が文書を取り出すことを求める要求を送信したとき、ＡＣＬをチェックしなければならない。要求元は、アクセスが許可されている場合、文書のコピーを与えられるだけである。

【００４７】本発明の好ましい実施形態によれば、要求元が、アクセス要求を実行する前に、自らの文書へのアクセスを検証できるようにするために機能リストを使用することができる。機能リストは、特定のユーザがアクセス特権を有するリポジトリ内のすべての文書を識別する。要求元の機能リストは、自分のヴォールト内に格納され維持される。要求元は、そのリストをチェックするだけで、どの文書にアクセスできるのかを判定する。機能リストの使用および維持については、図７に関連して下記で詳細に説明する。

【００４８】要求元が文書へのアクセスを許可されていない場合は、発信者にエラー・メッセージが戻され、システムに記録される（ブロック４１４）。

【００４９】図５に進むと、要求元が文書の受取りを許可されている場合、発信者のヴォールト・アプリケーションは文書を暗号解読し（ブロック４１６）、公証済み署名を検証する（ブロック４１８）。発信者のオリジナル署名は暗号化されていない文書内容に対して計算されたものであるため、文書内容にアクセスできる（すなわち発信者の秘密キーを有する）ユーザだけが署名を検証

することができる。この署名が、文書発信者が自分のファイル内に有するものと対応していない場合は、預けた文書と同じバージョンでないことが明らかなので、発信者はエラー・メッセージをアプリケーション・サーバに戻す（ブロック４２０）。

【００５０】署名が検証された場合、発信者は暗号解読された文書と公証済み署名を要求元のヴォールトに転送する（ブロック４２２）。

【００５１】暗号解読された文書を受信すると、要求元のヴォールト・アプリケーションは、発信者の公証済み署名の検証を試みる（ブロック４２４）。要求元がそれを検証できない場合、エラー・メッセージが発信者に戻され、システムに記録される（ブロック４２６）。

【００５２】発信者の公証済み署名が検証できる場合、要求元のヴォールトは文書と共に受け取った公証済み署名に署名する。この署名は公証済み署名ならびに現タイム・スタンプに対して計算され、要求元が文書をリポジトリから取り出したことを証明する非拒否証明を構成する（ブロック４２８）。要求元のヴォールトは、暗号解読された文書を生成した非拒否証明と共に要求元のデスクトップに戻す（ブロック４３０）。さらに要求元のヴォールトは、非拒否証明をアプリケーション・サーバのヴォールトに転送する（ブロック４３２）。アプリケーション・サーバは、これを受け取り次第、要求元ヴォールトの署名を検証する（ブロック４３４）。署名が検証できない場合、発信者にエラー・メッセージが戻されシステムに記録される（ブロック４３６）。署名が検証できる場合、後で要求元がこの文書を取り出したことをアプリケーション・サーバが証明しなければならない場合に使用するために、アプリケーション・サーバ・ヴォールトはこの証明をアプリケーション・データベースに格納する（ブロック４３８）。

【００５３】文書取出しに関するアクセス制御の不変性（immutability）前述のように、データ・リポジトリでは文書アクセス制御に関する要件がある。すなわち、文書の所有者が許可したユーザだけがその文書を閲覧することが可能であり、文書アクセス許可は、文書の所有者（すなわち文書発信者）と、所与の文書のアクセス制御リストを修正する許可を文書の所有者から与えられている他のユーザだけが修正できるということである。リポジトリ管理者でも、文書の所有者から許可されていない限り文書のアクセス許可を修正する権限のないことを保証することが重要である。

【００５４】文書アクセス制御の不変性のためのアプリケーションの要件には、２つの異なるタイプのものがある。文書アクセスは、

１）ユーザが閲覧する許可を与えられているすべての文書を見つけるための検索を実行するとき、および

２）ユーザが実際に文書の取出しを実行するときに、チェックする必要がある。

【００５５】すべてのアプリケーションは、文書取出し時にアクセス制御を実施する必要がある（上記アクセス・タイプの２）。このタイプのアクセスの場合、リポジトリは、文書のアクセス制御が、競合企業など許可されていないユーザによって修正される可能性がないことを保証しなければならない。

【００５６】ただし、一部のアプリケーションでは、閲覧を許可されているすべての文書についてユーザが文書リポジトリを照会できることが不可欠ではない。たとえば、この知識は業務会議の際にオフラインであるいは電話を介して伝えることができる。このような場合、ユーザはすでにどの文書にアクセスできるかを知っているため、要求元の自分の文書アクセスに関する知識は、リポジトリのアクションによって影響を受けることはない。

【００５７】文書の検索時ではなく文書の取出し時のみにアクセス制御の不変性を実施するシステムは、本発明者等が同時に提出した「System for Electronic Repositoryof Data Enforcing Access Control on Data Retrieval」という名称の出願（ＩＢＭ整理番号第ＣＡ９９８－０３０号）の主題である。このシステムでは、アクセス制御情報はアプリケーション・サーバのデータベース／リポジトリに格納される。

【００５８】ユーザが自分の文書アクセスに関する独立した情報を持っていない場合に使用できる、アクセス制御の不変性のより強力な形式は、文書検索と文書取出しの両方に関するものである。この要件を満たすために、アクセス制御情報はアプリケーション・データベース内には格納できず、その代わりに文書の所有者のヴォールトに格納される。このスキームが本発明の主題であって、図６ないし図８の流れ図に示し下記で説明する。

【００５９】好ましい実施形態では、各文書は、様々なユーザの文書に対するアクセス許可を識別する、それに関連付けられたアクセス制御リスト（ＡＣＬ）を有する。さらに、システムの各ユーザは、ユーザが所有していないけれどもアクセスすることのできるすべての格納文書を識別する機能リストを有する。

【００６０】不変性を保証するために、各ＡＣＬは、図６に示すように文書所有者のヴォールト内で処理され、これと平行して、各機能リストは、図７に示すように関連するユーザのヴォールト内で処理される。

【００６１】図６から始めると、ＡＣＬが更新されているとき（ブロック５００）、文書所有者のヴォールトはその変更によって影響を受けるユーザを決定し（ブロック５０２）、アクセス変更のタイプ（アクセスの追加、拡張、または制限）を識別するメッセージが、文書へのアクセスが修正された各ユーザのヴォールト内に寄託される（ブロック５０４）。

【００６２】各ＡＣＬには、その最新の修正のバージョン番号およびタイム・スタンプが付随する。したがって、文書所有者のヴォールトはＡＣＬのバージョン番号

を増分し（ブロック５０６）、それに関連付けられた古いタイム・スタンプが最新のタイム・スタンプで置き換えられる（ブロック５０８）。ＡＣＬの不変性を保証するためのトークンが、このときＡＣＬに関連付けられている現バージョン番号と現タイム・スタンプから作成され、文書発信者のヴォールトによって署名される（ブロック５１０）。ＡＣＬも、文書発信者のヴォールトによって署名される（ブロック５１２）。

【００６３】ＡＣＬトークンは、将来のＡＣＬ検証のためにユーザのアクセス・アプリケーションと共にデスクトップに格納するため、文書へのアクセスが許可されている任意のユーザのヴォールトへも転送される（ブロック５１４）。署名付きトークンは、格納のために文書発信者のデスクトップに転送される（ブロック５１６）。文書発信者は、署名付きトークンのコピーを保持しているので、文書ＡＣＬが最新のものであるか否かの最終決裁者となる。

【００６４】業務パートナが文書を取り出したいときは、ＡＳヴォールト・アプリケーションは、前述のように暗号化された文書を発信者のヴォールトに送信する（図４のブロック４０８）。要求元の許可を検証するために（図４のブロック４１２）、文書発信者のヴォールトは単に、検証されローカルに保管されたＡＣＬ内で、要求元が指定された文書に対するアクセス権を有することをチェックする。この方法を使用すると、アプリケーション・データベース内に格納されたＡＣＬを発信者のヴォールトに検出されずに修正することはまったくできない。

【００６５】前述のように、リポジトリ内の文書を所有している各ユーザは、各ＡＣＬの正しいバージョンの署名付きトークンをそのデスクトップ上に保持している。ユーザ・ヴォールトによって保持されているＡＣＬバージョンは、ユーザのデスクトップ上に格納されている署名付きトークンとユーザのヴォールト内に格納されているそれとを比較することによって検証される。この比較は、様々なときに実行することができる。ユーザのヴォールト内に格納されているＡＣＬを検証する好機の１つはログオン時であり、ユーザがログオンするごとにユーザのＡＣＬが検証される。

【００６６】ＡＣＬ検証に失敗した場合、ユーザのヴォールト・アプリケーションは、ＡＣＬによって保護されている文書を取り出すことを求めるすべての要求の受付けを自動的に停止する。このような文書のアクセス不能状態は、ユーザが新しいＡＣＬを作成するか、または既存のＡＣＬを再認証するまで持続する。既存のＡＣＬの再認証プロセスには、ユーザのヴォールトに格納されたＡＣＬトークンとユーザのデスクトップ上に格納されたトークンとの同期化が含まれる。

【００６７】ＡＣＬが更新されたとき、図６に示したステップと平行していくつかのステップが実行される。この追加ステップを図７に示す。

【００６８】各ユーザのヴォールトは、ユーザがアクセスできるすべての文書のリストを含む機能リストの維持を担当する。機能リスト自体の現在性（currency）は、バージョン番号および最新のタイム・スタンプによって識別される。つまり、ユーザが文書にアクセスできる能力の修正（文書ＡＣＬの更新）を示すメッセージがユーザのヴォールトに着信すると（ブロック５２０）、ユーザ・ヴォールト内の機能リストはバージョン番号（ブロック５２２）および最新のタイム・スタンプ（ブロック５２４）によって自動的に更新される。機能リストの正確さを検証する際に使用できるそのトークンが、バージョン番号およびタイム・スタンプに対して計算される（ブロック５２６）。このトークンは、ユーザのヴォールトによって署名され（ブロック５２８）、機能リストも同様に署名される（ブロック５３０）。署名されたトークンと機能リストは、どちらもユーザのヴォールトに格納されるが（ブロック５３２）、更新が行えるようになるまでこの古い機能リストのトークンはユーザのデスクトップ上に格納されたトークンと対応しているので、ユーザのヴォールトは古い機能リストとそれに関連付けられたトークンを保存する。

【００６９】現在の機能リストをデスクトップ上に格納された対応するユーザのトークンと同期化させる１つの方法は、ユーザがログオンした際に自動的に同期化させるものである（ブロック５３２）。ユーザのデスクトップにあるトークンの正確さは、ユーザのヴォールト内に保存されている古いトークンと突き合わせてチェックすることができ、次いでこの更新されたトークンをユーザのデスクトップに送信することができる（ブロック５３４）。ユーザのデスクトップ上で古いトークンが置き換えられた後、古い機能リストおよびそれに関連付けられたトークンをユーザのヴォールトから削除することができる。

【００７０】ユーザのデスクトップ上にある機能リスト・トークンを更新する代替方法（図示せず）は、最後にログオンした後に行った機能リストへの更新の検討を、自発的に行うようにユーザに要求することである。

【００７１】ＡＣＬと機能リストを確実に一致させるためには、システムの基礎となっている環境（たとえばＩＢＭ Vault Registry製品）が、ヴォールト間で寄託されたメッセージに対して保証されたメッセージ送達を提供しなければならない。機能更新の送達の保証は、たとえば、更新を受け取ったユーザに受領証を要求することによりアプリケーションが行うこともできる。

【００７２】このスキームの結果、ＡＣＬおよび機能リストはすべてそれぞれの所有者によって格納される。システム内のどの当事者も、文書所有者が変更に気付くことなく、文書のアクセス制御リストを変更することはできない。さらに、システム内のどの当事者も、許可され

たユーザが変更に気付くことなく、文書へのアクセスに関するユーザの知識（すなわち機能）を変更することはできない。

【００７３】検索がアプリケーション・サーバのヴォールトによって実行される、本発明者の前掲の同時係属出願に記載されたアクセス制御スキームとは違って、本発明によれば、ユーザがアクセスを許可されている文書の検索は、ユーザ自身のヴォールト・アプリケーションによって実行される。

【００７４】所有者特権の割当て環境によっては、文書所有者が他の人に所与の文書のアクセス・リストの修正を許可できるようにする必要がある。たとえば、所有者が使用できない場合、別の許可されたユーザが所与の文書のアクセス制御を更新できるようになる。

【００７５】本発明の好ましい実施形態によれば、ＡＣＬまたは機能リストの更新は、図８に示したステップに従ってシステム内の他のユーザが実行することができる。

【００７６】例えばＡＣＬの更新を試みるとき、更新を行うユーザは、そのＡＣＬの最新の署名付きトークンを提示することができなければならない（ブロック６００）。署名付きトークンは、更新を行うユーザ自身のヴォールトに送信され（ブロック６０２）、それが署名付きトークンを発信者のヴォールトに渡す（ブロック６０４）。更新を行うユーザがこの文書のＡＣＬに割り当てられた所有者特権を持っていない場合、文書発信者のヴォールトはこれを検出して、更新を拒否し、ユーザのヴォールトにエラー・メッセージを戻す（ブロック６０８）。

【００７７】発信者のヴォールトが署名を行うユーザの文書へのアクセスを検証できる場合、およびＡＣＬトークンのバージョン番号とタイム・スタンプが最新のものである場合（ブロック６０６）、ＡＣＬは更新され（ブロック６１０）、新しいトークンが生成され署名されて（ブロック６１２）、発信者のヴォールトに格納される（ブロック７１４）。この新しい署名付きトークンは、更新元のヴォールトに送信される（ブロック６１６）。この更新元のヴォールトは、新しいトークンを格納するために更新元のデスクトップに戻す（ブロック６１８）。新しい署名付きトークンはまた、リポジトリに格納するために任意選択でアプリケーション・サーバのヴォールトに転送することもできる（ブロック６２０）。

【００７８】この手順には、ＡＣＬの更新を実行できる人が常に１人だけであることが必要である。たとえば、文書所有者のジョン（John）が休暇で休む場合、彼は同僚のメアリー（Mary）に、文書のＡＣＬに関する彼の最新のトークンを与えることによって、彼が会社を休んでいる間に彼女が彼の文書のＡＣＬを更新できるように許可することができる。次いでメアリーは、自分のヴォールトを介してジョンのヴォールトにトークンを提示することによって、ＡＣＬの更新を発行する。メアリーは、このＡＣＬの新しい署名付きトークンを受け取り、ジョンが会社に復帰したとき彼に戻す。この新しいトークンをインストールした後、ジョンは自分自身のＡＣＬ更新を発行することができる。

【００７９】データのバックアップおよび回復

文書リポジトリの管理者が、以前のバックアップから文書データベースを復元する必要が生じることが時折ある。これはたとえば、ディスク・クラッシュなど破局的なデータベースの障害が生じた場合に必要になる。

【００８０】バックアップに含める必要のあるデータは、文書自体、ＡＣＬ（アプリケーション・データベースまたは所有者ヴォールトのどちらに格納されている場合でも）、機能リスト（前述のように機能を実行するシステムに関する）、ＡＣＬの検証トークン、および機能リストである。データを復元した後、最新のバックアップ後に実行された更新は失われることがある。本発明では、ＡＣＬおよび機能リストの更新がそれに含まれる可能性がある。その場合、ユーザのデスクトップに格納された検証トークンが、対応するヴォールト内のトークンと一致しなくなり、適正なユーザ・アクセスが拒否されることがある。

【００８１】したがって、様々な状況でデータを復元する場合の標準を提供するために、以下のシステムが実装された。バックアップはタイム１で実行され、復元はその後のタイム２で発生したと仮定する。

【００８２】ヴォールトに格納された文書データベース、ＡＣＬ、機能リスト、および対応するトークンの完全なデータ復元が実行される場合、タイム１より前に文書へのアクセスを許可されているユーザは、タイム２の後にもこれにアクセスできる。つまり、ユーザがタイム１より前には許可されていて、タイム１より後でタイム２より前にその権限が取り消された場合、そのユーザは、文書発信者がＡＣＬトークンのチェックを実行するまでは文書にアクセスできることになる。したがって、すべてのユーザは、完全なデータ復元の後に、ＡＣＬおよび機能リストのチェックを行う必要がある。

【００８３】文書データベースのみが復元され、ＡＣＬ、機能リスト、およびヴォールトに格納されたトークンはそのままである場合、ユーザは、タイム１より後に追加されたが、その後データベースの復元中に失われたため、データベース内に存在しない文書へのアクセスが許可されていることを発見することがある。すべてのトークンは最新のものであるため、他の異常はいっさい発生しない。

【００８４】別のケースとして、機能リストは使用されていないが、ＡＣＬがアプリケーション・データベースに格納されているシステムの場合がある。文書データベースおよびＡＣＬが復元されており、ヴォールトに格納されたトークンは復元されていない場合、ユーザは、タ

イム１より後に変更されたＡＣＬを有するすべての文書がアクセス不可能であることを発見する。これは、アプリケーション・データベース内のＡＣＬトークンが、個々の所有者のヴォールト内に格納されているトークンと一致しないためである。この問題を処理するためには、すべての文書発信者がＡＣＬを更新しなければならない。その一方法としては、管理者が古いＡＣＬ（タイム１の時点では有効であった）を文書所有者に送信し、対応するトークンをそのヴォールトに再インストールするように依頼することである。この更新は自動ではなく手動で実行され、所有者がこの更新を完了するまで所有者の文書はアクセス不能である。

【００８５】データベースの不整合を避けなければならない場合、リポジトリ管理者は復元後、発信者が是正処置を実行するまで、すべての文書へのアクセスを禁止することができる。このアクセス禁止は、リポジトリ内に格納されているすべての文書に適用されるか、または整合性がクリティカルな文書のサブセットだけに適用される。この場合、リポジトリ管理者に依拠して、システムの整合性を保持しなければならない。ただし前述のように、いずれの場合でも管理者には文書へのユーザ・アクセスを認可したり取り消したりする権限はもたない。

【００８６】以上、IBM Vault Registry製品を使用して実装された本発明の好ましい実施形態について述べてきた。ただし本発明が、各ユーザのデスクトップにローカルに配置された安全なヴォールト様環境など、類似の機能を提供する他の製品を使用しても実装できることは、当業者には自明であろう。この性質および当業者に自明な他の性質の修正は、添付の特許請求の範囲によってカバーされるものとする。

【００８７】まとめとして、本発明の構成に関して以下の事項を開示する。

【００８８】（１）データ・リポジトリ・システムに格納された電子データ・ファイルを検索するための安全なシステムであって、（ｉ）データ・リポジトリ・システム内にある電子データ・ファイルの寄託側コンピュータ用の第１のエージェント・プログラムと、（ｉｉ）電子データ・ファイルへのアクセス特権を有する第１のユーザ・コンピュータ用の第２のエージェント・プログラムとを収容する通信環境と、前記第１のエージェント・プログラムによってアクセス可能であり維持され、電子データ・ファイルに関するアクセス制御をリストした電子データ・ファイルの目録と、前記第２のエージェント・プログラムによってアクセス可能であり維持され、電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権に関する第１の記録と、電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、第１の記録を更新するため、前記第１のエージェント・プログラムから前記第２のエージェント・プログラムへ伝える手段と、電子データ・ファイルが前記第２のエージェント・プログラムに解放される前に、前記第１のエージェント・プログラムが電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権を検証するための手段とを含むシステム。

（２）前記第１のエージェント・プログラムが寄託側コンピュータの安全な拡張であり、前記第２のエージェント・プログラムが第１のユーザ・コンピュータの安全な拡張である、上記（１）に記載の安全なシステム。

（３）電子データ・ファイルに対する前記第１のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、前記第２のエージェント・プログラムから第１のユーザ・コンピュータへ伝える手段をさらに含む、上記（２）に記載の安全なシステム。

（４）電子データ・ファイルに対するアクセス特権を有する第２のユーザ・コンピュータ用の第３のエージェント・プログラムと、前記第３のエージェント・プログラムによってアクセス可能であり維持され、電子データ・ファイルに対する第２のユーザ・コンピュータのアクセス特権に関する第２の記録とを含み、第１の記録を更新するために、電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、前記第１のエージェント・プログラムから前記第２のエージェント・プログラムへ伝える手段が、第２の記録を更新するために、電子データ・ファイルに対する第２のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、前記第１のエージェント・プログラムから前記第３のエージェント・プログラムに伝える手段を含み、電子データ・ファイルが前記第２のエージェント・プログラムに解放される前に、前記第１のエージェント・プログラムが電子データ・ファイルに対する第１のユーザ・コンピュータのアクセス特権を検証するための手段が、電子データ・ファイルが前記第３のエージェント・プログラムに解放される前に、前記第１のエージェント・プログラムが電子データ・ファイルに対する第２のユーザ・コンピュータのアクセス特権を検証するための手段を含む、上記（１）または（２）にいずれか一項に記載の安全なシステム。

（５）前記第３のエージェント・プログラムが前記第２のユーザ・コンピュータの安全な拡張である、上記（４）に記載の安全なシステム。

（６）電子データ・ファイルに対する前記第２のユーザ・コンピュータのアクセス特権に影響を与える目録の変更を、前記第３のエージェント・プログラムから前記第２のユーザ・コンピュータに伝える手段をさらに含む、上記（５）に記載の安全なシステム。

（７）通信環境がサーバを含む、上記（２）または（５）に記載の安全なシステム。

（８）前記通信環境に収容されたデータ・リポジトリ・システムへのインタフェースをさらに含み、前記インタ

フェースがデータ・リポジトリ・システムおよびエージェント・プログラムとの間の双方向通信をすべて受け取るように適合されている、上記（１）、（２）、または（５）のいずれか一項に記載の安全なシステム。

（９）前記インタフェースが前記データ・リポジトリ・システムの安全な拡張である、上記（８）に記載の安全なシステム。

（１０）電子データ・リポジトリ用の安全な電子データ検索システムを維持する方法であって、前記システムが、データ・リポジトリ内に格納された各電子データ・ファイルに関するアクセス制御をリストした目録と、リポジトリ内に格納された電子データに対するアクセス権を有する各コンピュータの文書アクセス特権をリストした記録とを有し、リポジトリ内に格納されている電子データ・ファイルに関する目録を更新するステップと、前記更新によって電子データ・ファイルへのアクセスが変更されたすべてのコンピュータを識別するステップと、前記アクセスの変更を影響されるすべてのコンピュータに伝えるステップと、影響されるすべてのコンピュータのアクセス特権記録を更新するステップと、前記更新されたアクセス特権記録を前記影響されるコンピュータに伝えるステップとを含む方法。

（１１）データ・リポジトリ・システム内に格納された電子データ・ファイルを検索するための安全なシステムであって、データ・リポジトリ・システム内に格納された各電子データ・ファイルに関するアクセス制御をリストした目録を維持する手段と、各目録へのアクセスを割当特権を有するコンピュータだけに制限する手段と、データ・リポジトリ・システム内の少なくとも１つの電子データ・ファイルへのアクセス特権を有する各コンピュータに関連付けられた電子データ・ファイルに対するアクセス特権をリストした記録を維持する手段と、前記各記録に対するアクセスを前記アクセス特権を有する関連するコンピュータだけに制限する手段と、目録のアクセス変更によって影響を受ける各コンピュータに関連付けられた前記記録を更新する手段とを含むシステム。

（１２）上記（１０）に記載の方法をコンピュータで実行する際に使用するための命令を格納するコンピュータ可読メモリ。

【図面の簡単な説明】

【図１】第三者保管者を利用する文書リポジトリ・システムの概略図である。

【図２】図１と同様、本発明の好ましい実施形態で使用されるヴォールト文書リポジトリ・システムを示す概略図である。

【図３】本発明による文書作成のプロセスを示す流れ図である。

【図４】本発明による文書検索のプロセスを示す流れ図である。

【図５】本発明による文書検索のプロセスを示す流れ図である。

【図６】本発明の好ましい実施形態による、文書検索に関するアクセス制御の不変性を提供するためのプロセスを示す流れ図である。

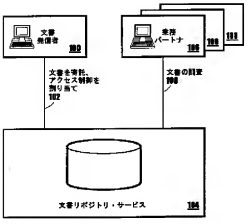
【図７】本発明の好ましい実施形態による、文書検索に関するアクセス制御の不変性を提供するためのプロセスを示す流れ図である。

【図８】本発明による格納文書に所有者特権を割り当てるためのプロセスを示す流れ図である。

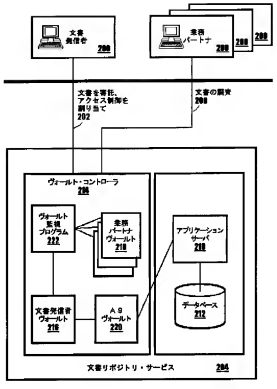
【符号の説明】

２００　文書発信者
２０２　文書の書託、アクセス制御の割当て
２０４　文書リポジトリ・サービス
２０６　業務パートナ
２０８　文書の調査
２１０　アプリケーション・サーバ
２１２　データベース・リポジトリ
２１４　ヴォールト・コントローラ
２１６　文書発信者ヴォールト
２１８　業務パートナ・ヴォールト
２２０　ＡＳヴォールト
２２２　ヴォールト監視プログラム

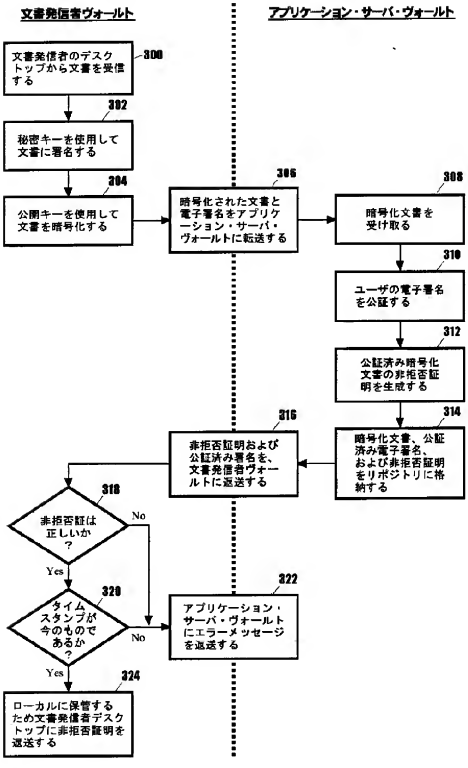
【図１】


文書
所有者
190
業界
パートナ
195
191
文書を寄託、
アクセス制御を
割り当て
192
文書の調査
200
文書リポジトリ・サービス
194

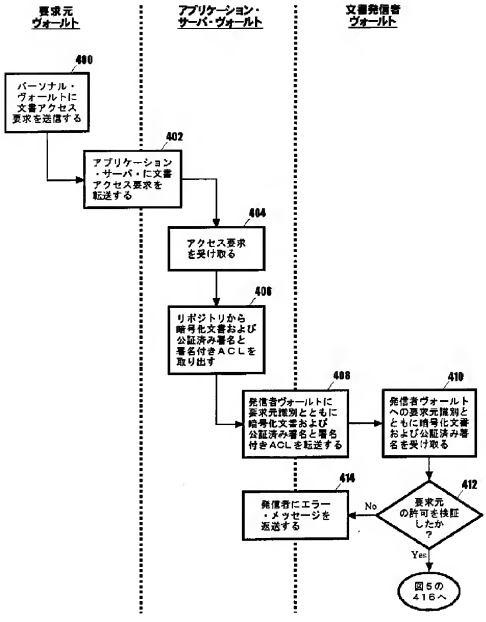
【図２】


文書
所有者
290
業界
パートナ
295
291
文書を寄託、
アクセス制御を
割り当て
292
文書の調査
300
ヴォールト・コントローラ
296
ヴォールト
処理
プログラム
227
業界
パートナ
ヴォールト
218
アプリケーション
サーバ
216
文書所有者
ヴォールト
219
ＡＳ
ヴォールト
220
データベース
212
文書リポジトリ・サービス
294

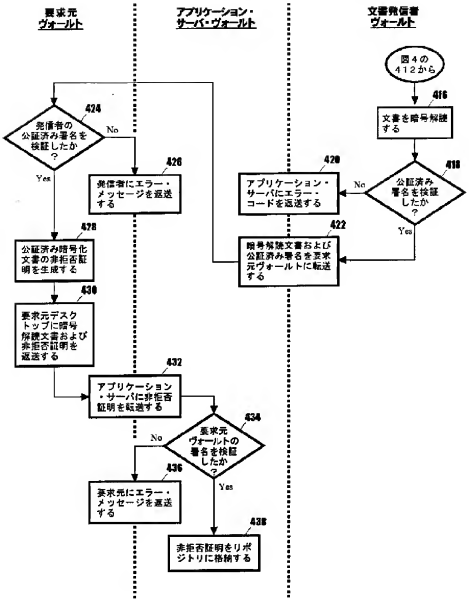
【図３】


文書発信者ヴォールト
アプリケーション・サーバ・ヴォールト
300
文書発信者のデスクトップから文書を受信する
302
秘密キーを使用して文書に署名する
304
公開キーを使用して文書を暗号化する
306
暗号化された文書と電子署名をアプリケーション・サーバ・ヴォールトに転送する
308
暗号化文書を受け取る
310
ユーザの電子署名を公証する
312
公証済み暗号化文書の非拒否証明を生成する
314
暗号化文書、公証済み電子署名、および非拒否証明をリポジトリに格納する
316
非拒否証明および公証済み署名を、文書発信者ヴォールトに返送する
318
非拒否証は正しいか？
No
Yes
320
タイムスタンプが今のものであるか？
No
Yes
322
アプリケーション・サーバ・ヴォールトにエラーメッセージを返送する
324
ローカルに保管するため文書発信者デスクトップに非拒否証明を返送する

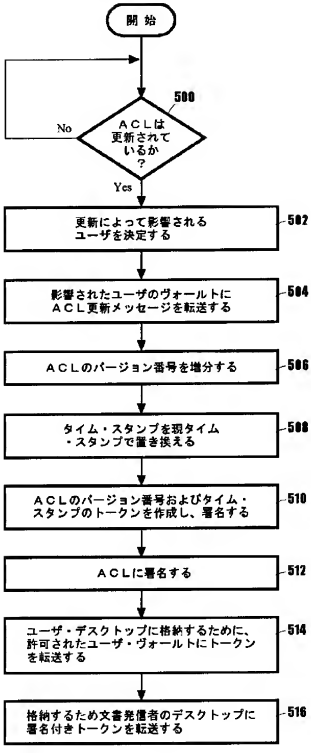
【図４】


要求元
ヴォールト
アプリケーション・
サーバ・ヴォールト
文書発信者
ヴォールト
400
パーソナル・
ヴォールトに
文書アクセス
要求を送信する
402
アプリケーション
・サーバ・に文書
アクセス要求を
転送する
404
アクセス要求
を受け取る
406
リポジトリから
暗号化文書および
公証済み署名と
署名付きＡＣＬを
取り出す
408
発信者ヴォールトに
要求元識別とともに
暗号化文書および
公証済み署名と署名
付きACLを転送する
410
発信者ヴォールト
への要求元識別と
ともに暗号化文書
および公証済み署
名を受け取る
412
要求元
の許可を検証
したか
？
No
Yes
414
発信者にエラー
・メッセージを
返送する
図５の
４１６へ

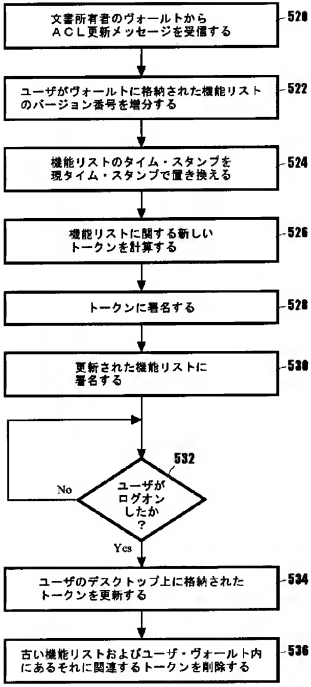
【図５】


要求元
ヴォールト
アプリケーション・
サーバ・ヴォールト
文書発信者
ヴォールト
図４の
412から
416
文書を暗号解読
する
418
公証済み
署名を検証
したか
？
No
Yes
420
アプリケーション・
サーバにエラー・
コードを返送する
422
暗号解読文書および
公証済み署名を要求
元ヴォールトに転送
する
424
発信者の
公証済み署名を
検証したか
？
No
Yes
426
発信者にエラー・
メッセージを返送
する
428
公証済み暗号化
文書の非拒否証
明を生成する
430
要求元デスク
トップに暗号
解読文書および
非拒否証明を
返送する
432
アプリケーション
・サーバに非拒否
証明を転送する
434
要求元
ヴォールトの
署名を検証
したか
？
No
Yes
436
要求元にエラー・
メッセージを返送
する
438
非拒否証明をリポ
ジトリに格納する

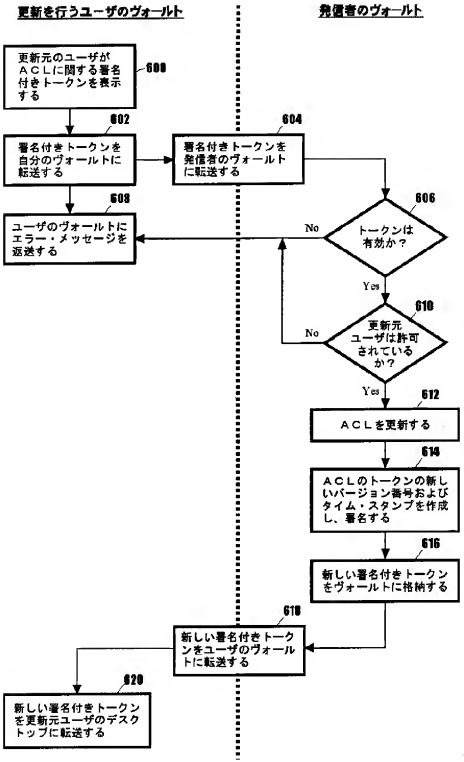
【図６】


開始
500
ＡＣＬは更新されているか？
No
Yes
更新によって影響されるユーザを決定する
502
影響されたユーザのヴォールトにＡＣＬ更新メッセージを転送する
504
ＡＣＬのバージョン番号を増分する
506
タイム・スタンプを現タイム・スタンプで置き換える
508
ＡＣＬのバージョン番号およびタイム・スタンプのトークンを作成し、署名する
510
ＡＣＬに署名する
512
ユーザ・デスクトップに格納するために、許可されたユーザ・ヴォールトにトークンを転送する
514
格納するため文書発信者のデスクトップに署名付きトークンを転送する
516

【図７】


文書所有者のヴォールトから
ＡＣＬ更新メッセージを受信する
520
ユーザがヴォールトに格納された機能リスト
のバージョン番号を増分する
522
機能リストのタイム・スタンプを
現タイム・スタンプで置き換える
524
機能リストに関する新しい
トークンを計算する
526
トークンに署名する
528
更新された機能リストに
署名する
530
532
ユーザが
ログオン
したか
？
No
Yes
ユーザのデスクトップ上に格納された
トークンを更新する
534
古い機能リストおよびユーザ・ヴォールト内
にあるそれに関連するトークンを削除する
536

【図８】


更新を行うユーザのヴォールト
発信者のヴォールト
更新元のユーザがＡＣＬに関する署名付きトークンを表示する
600
602
署名付きトークンを自分のヴォールトに転送する
604
署名付きトークンを発信者のヴォールトに転送する
606
トークンは有効か？
No
608
ユーザのヴォールトにエラー・メッセージを返送する
Yes
610
更新元ユーザは許可されているか？
No
Yes
612
ＡＣＬを更新する
614
ＡＣＬのトークンの新しいバージョン番号およびタイム・スタンプを作成し、署名する
616
新しい署名付きトークンをヴォールトに格納する
618
新しい署名付きトークンをユーザのヴォールトに転送する
620
新しい署名付きトークンを更新元ユーザのデスクトップに転送する

(72)発明者　ハミド・バチャ
アメリカ合衆国22066　バージニア州グレート・フォールズ　ローカスト・ヒル・ドライブ　9510
(72)発明者　ロバート・ブルース・キャロル
アメリカ合衆国10549　ニューヨーク州マウント・キスコ　バイラム・レーク・ロード　246
(72)発明者　レフ・ミルラス
カナダ　エル４ジェイ　６ピー４　オンタリオ州ソーンヒル　ミルクロフト・ウェイ　98
(72)発明者　スン・ウェイ・チャオ
カナダ　エム２エヌ　３ケイ５　オンタリオ州トロント　ホリウッド・アベニュー　168